Chapitre VIII

Cryptologie
Partie II

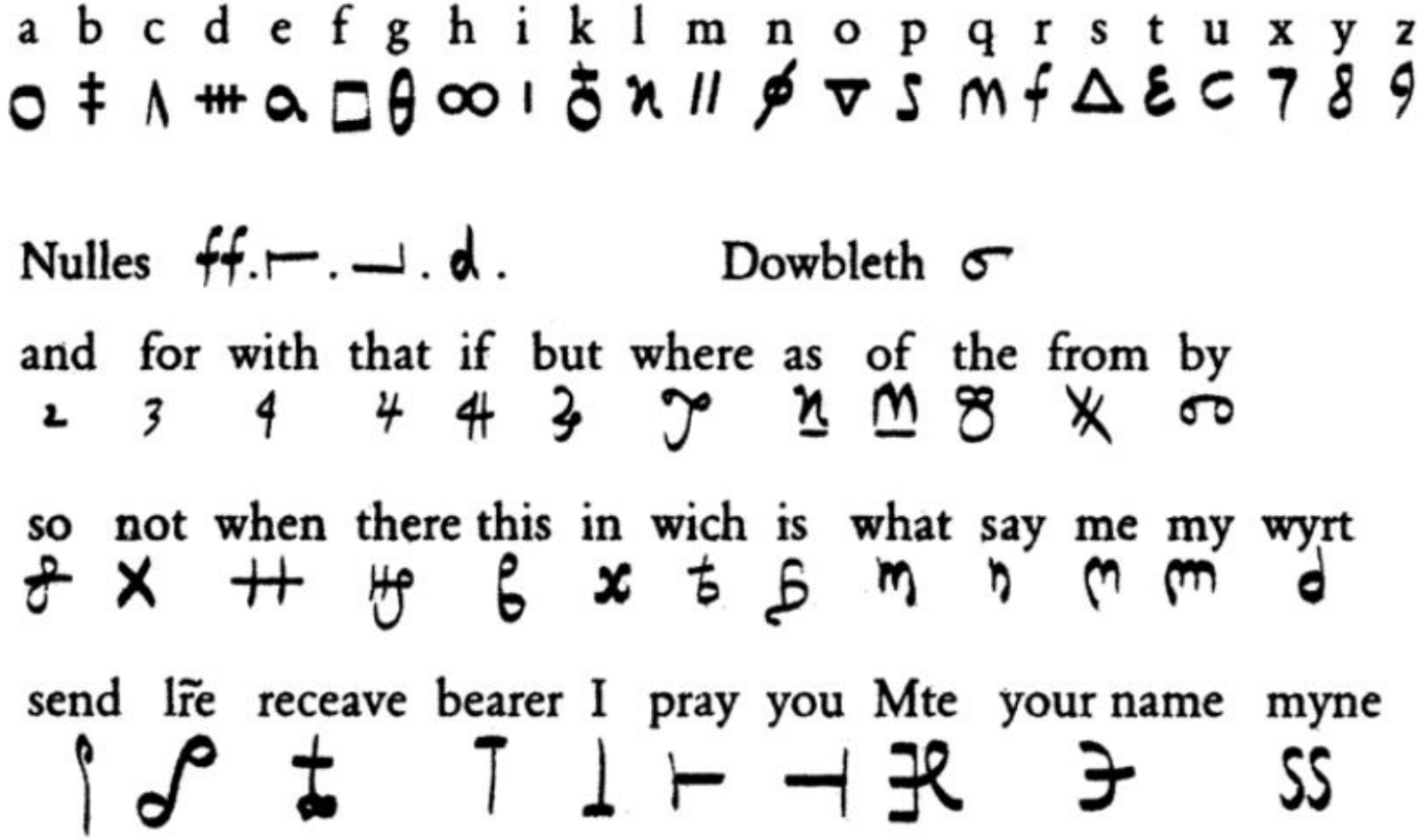
Substitution alphabétique

La substitution réputée inviolable … ne l'est plus vraiment.

Il fallait renforcer le cryptage:

- Introduction d'éléments nuls: on chiffre l'alphabet avec des codes de 01 à 99. Les codes non utilisés sont introduits aléatoirement dans le texte. Cela complique l'analyse de fréquence
- Introduction de mots-clés en plus de la substitution alphabétique
- Introduction de caractères autres que les lettres et les chiffres (on chiffre aussi la ponctuation par exemple)

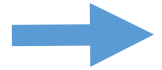
Code Mary Stuart



Substitution homophonique

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
12	81	13	01	06	31	25	39	32	15	04	26	22	18	00	38	94	29	11	17	02	34	60	28	24	01
33		41	03	10				50			37	27	58	05	90		35	19	20	08	52				
47		62	45	14				56			51	68	59	07	95		40	21	30	61					
48				16				70			65		66	54			42	36	43	63					
53				23				73			84		71	72			77	76	49	85					
67				24				83					91				80	86	69	90					
78				44				88					99					96	75						
92				46				93										97							
				54																					
				55																					
				57																					
				74																					
				79																					
				82																					
				87																					
				98																					

Chaque lettre se voit assigner un certain nombre de codes en fonction de sa fréquence dans la langue. Le « e » reçoit donc 16 codes différents. A chaque fois qu'il faut coder un « e », on prend à tour de rôle chacun des 16 codes qui représentent la lettre.



On déjoue l'analyse de fréquence. La fréquence de chaque caractère est ramenée à une même valeur

Substitution homophonique

Cependant à l’aide de la linguistique, on peut constater que certaines lettres apparaissent toujours suivies par une ou plusieurs lettres qui sont toujours les mêmes.

Exemple: le « q » est toujours suivi du « u ».

Vigenère

Au XVe siècle, Léon Battista Alberti suggéra d'utiliser plusieurs alphabets chiffrés et d'en alterner l'usage au cours du cryptage

Alphabet clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alphabet chiffré 1	F	Z	B	V	K	I	X	A	Y	M	E	P	L	S	D	H	J	O	R	G	N	Q	C	U	T	W
Alphabet chiffré 2	G	O	X	B	F	W	T	M	Q	I	L	A	P	Z	J	D	E	S	V	Y	C	R	K	U	H	N

Vigenère

Pour crypter le mot *hello -> AFPAD*

- On remplace le h par A (1er alphabet)
- On remplace le e par F (2e alphabet)
- On remplace le l par P (1er alphabet)
- On remplace le l par A (2e alphabet)
- On remplace le o par D (1er alphabet)

Alphabet clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alphabet chiffré 1	F	Z	B	V	K	I	X	A	Y	M	E	P	L	S	D	H	J	O	R	G	N	Q	C	U	T	W
Alphabet chiffré 2	G	O	X	B	F	W	T	M	Q	I	L	A	P	Z	J	D	E	S	V	Y	C	R	K	U	H	N

Vigenère

Malheureusement Alberti ne put terminer ces travaux …

Ce n’est que plus tard, que Blaise de Vigenère mit au point un code aboutit

Vigenère

Il est basé sur ce qu'on appelle le carré de Vigenère

Il reprend les 26 alphabets disponibles selon le chiffre de César

Et se base sur un mot clé connu de l'expéditeur et du destinataire

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Vigenère

Imaginons que le mot clé est ROUGE

On veut crypter «cryptanalyse »

Mot clé	R	O	U	G	E	R	O	U	G	E	R	O
Texte clair	c	r	y	p	t	a	n	a	l	y	s	e
Texte crypté	T	F	S	V	X	R	B	U	R	C	J	S

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Vigenère

Etonnamment, le chiffre de Vigenère ne fut pas adopté tout de suite.

On lui préféra tout d'abord des variantes des substitutions alphabétiques, comme la substitution homophonique.

Et ce chiffre polyalphabétique résista à la cryptanalyse pendant presque 300 ans.

Babage

Le chiffre de Vigenère était réputé « indéchiffrable »

Au XIXe siècle, Charles Babage qui est connu pour avoir posé les bases de l ’ordinateur moderne « cassa » le chiffre de Vigenère

Son analyse est basée sur le fait que malgré le nombre assez important de codage d’une même lettre, dans un texte assez long, des petits mots comme ET, LE, LA, LES, … vont invariablement entrainer la répétition des mêmes combinaisons de lettres plusieurs fois dans le message crypté

Babage

Exemple, utilisons le mot clé KILO pour crypter

‘the russe, the jasmin, the chine’

K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K	I	L	O	K
t	h	e	r	u	s	s	e	t	h	e	j	a	s	m	i	n	t	h	e	c	h	i	n	e
D	**P**	**P**	F	E	A	D	S	**D**	**P**	**P**	X	K	A	X	W	X	B	S	S	M	P	T	B	O

Babage

La répétition de certaine suite de lettre donne une indication sur la taille du mot clé.

A partir de là, on peut recommencer à faire des analyses de fréquence

Vigenère – Clé aléatoire

Vers la fin de la Première Guerre mondiale, le major Joseph Mauborgne (département de cryptographie de l'armée américaine) introduisit le concept de clé aléatoire.

Le principe repose sur l'utilisation d'une clé composée d'une suite de lettre au hasard

L'idée était de disposer de 2 épais blocs de papier dont chacune des centaines de pages portait une seule clé sous la forme de lettre alignée

Vigenère – Clé aléatoire

L’expéditeur crypte son message avec la clé de la première page

Le destinataire décrypte le message avec la clé de la première page

L’expéditeur et le destinataire détruise la première page

Et ensuite, on passe à la deuxième page …

Vigenère – Clé aléatoire

Ce chiffre ne permet plus l'attaque selon la méthode de Babage. En effet, il n'y a plus de répétition de la clé.

Ce chiffre est jugé comme d'une sureté absolue. C'est le Graal de la cryptographie

…

Vigenère – Clé aléatoire

En pratique, ce chiffre souffre de 2 inconvénients majeurs:

- Il faut établir une quantité astronomique de clés pour pouvoir gérer le trafic important (certainement en temps de guerre au sein d'une armée)
- Les recueils de clé étaient tapés à la machine par des êtres humains. Et les dactylos étaient entrainés à taper certaines lettres avec la main droite et d'autre avec la main gauche. En alternant main droite et main gauche, on n'est plus totalement aléatoire et on crée une sorte de schéma

Enigma

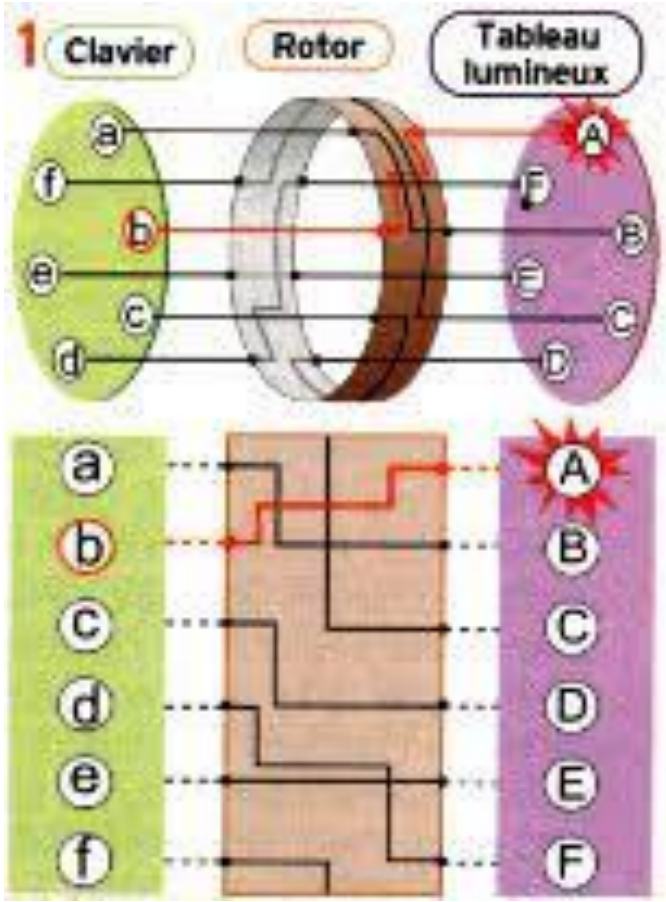
Arthur Scherbius développa une machine qu'il nomma Enigma et qui s'avéra être une arme redoutable pour les cryptographes

Enigma

On tape sur le clavier une lettre

En fonction du circuit électrique fournit par le rotor, une autre lettre s'allume

Le rotor effectue une rotation d'1/26^{e} de tour



Enigma

B donne A … Le rotor tourne

B donne C … Le rotor tourne

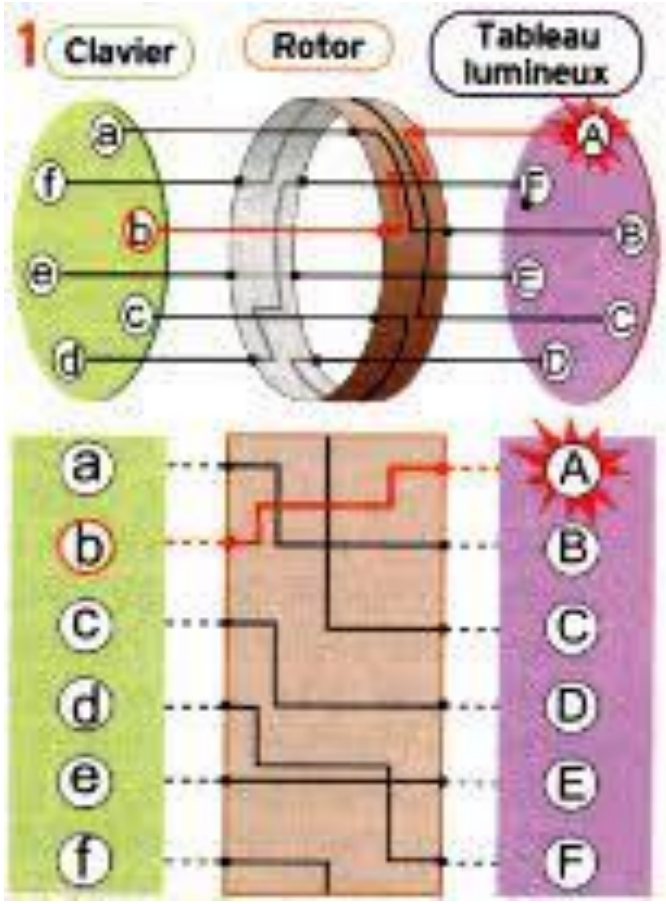
B donne E … Le rotor tourne

B donne B … Le rotor tourne

B donne D … Le rotor tourne

B donne C … Le rotor tourne

BBBBBB donne ACEBDC



Enigma

Défaut de ce système, au bout d'un tour complet du rotor, on recommence au début …

Ce qui introduit une répétition qui est bien souvent la faiblesse d'un chiffre

Un rotor offre 26 alphabets (en modifiant la position de départ)

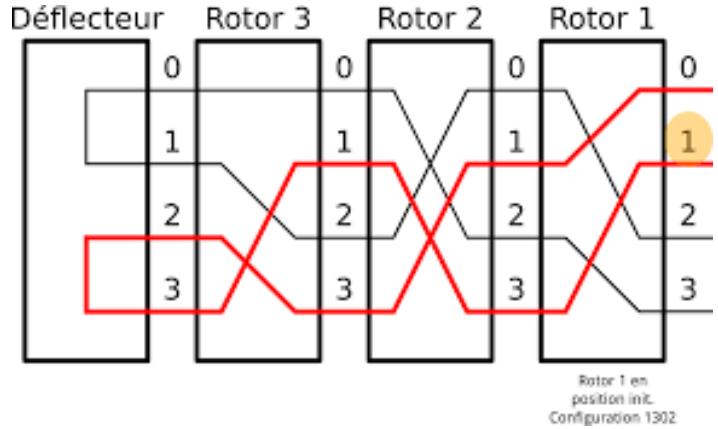
Scherbius introduisit un 2^{e} rotor ce qui permit d'augmenter à 676 le nombre d'alphabets possibles

Enigma

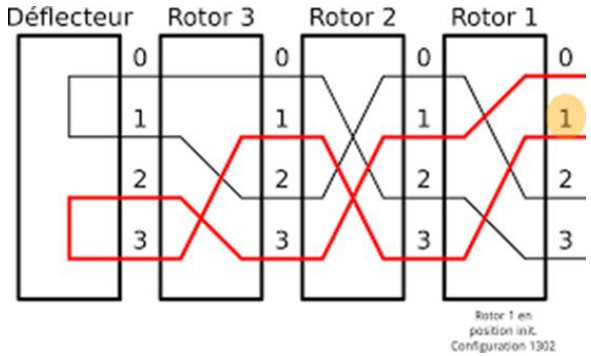
Ce n’était pas encore assez, on introduisit un 3^{e} rotor

-> Nombre d’alphabet: 17576

Ensuite on ajouta un réflecteur: c’est comme un tambour, mais il est fixe. De plus il renvoie le signal à travers les 3 rotors mais selon un chemin différent



Enigma



Le réflecteur n'augmente pas la complexité du chiffre, mais il offre un avantage d'utilisation
La machine peut être utilisée pour crypter et décrypter avec les mêmes réglages.

Je tape 0 ……. Il sort 1
J'envoie mon message au destinataire
Il met les rotors dans la même position que moi
Il tape 1 …… Il sort 0

L'envoyeur tape le message en clair pour obtenir le message crypté
Le destinataire tape le message crypté pour obtenir le message en clair

Enigma

17576 alphabets, ce n’est pas encore assez

Les rotors étaient mobiles et interchangeables. Ce qui offre 6 combinaisons différentes de position des rotors -> 17576 x 6 = 105456

Enigma

Enfin, on introduisit un tableau de connexions à fiches entre le clavier et le premier brouilleur. Ces connexions permettent d'échanger des lettres entre elles. On disposait en général de 6 fils qui permettait d'intervertir 6 paires de lettres -> 17576 x 6 x 100 391 791 500

≈ 10 000 000 000 000 000 clés possibles

Enigma

Enigma dans ses différentes versions représentait un code considéré comme inviolable

….

Jusqu’à ce qu’on trouve le moyen de le « casser »

Enigma

Rejewski et ses bombes ont exploités la répétition du code de chiffrement.

Il trouva le moyen de ne pas s'occuper des connexions par fiche, mais seulement de la position des brouilleurs

Il passa d'un problème à 10 000 000 000 000 000 à un problème à 105456 clés

Il introduisit aussi la mécanisation du décryptage en utilisant une machine qui lui permettait de parcourir les différentes possibilités automatiquement:

Bombes

Enigma

Les services de cryptanalyse anglais poursuivirent les travaux polonais pendant la Seconde Guerre mondiale.

Ils exploitèrent les faiblesses générées par les opérateurs:

- Utilisation répétée du même code personnel par facilité
- Utilisation des initiales de la petite amie de l'opérateur ou autre éléments personnels
- Utilisation des mots probables

Enigma

Alan Turing développe un moyen de trouver la clé du jour d'Enigma en combinant les erreurs des opérateurs avec une étude approfondie du fonctionnement interne de la machine

Il développe des versions améliorées des « bombes » qui permettent de mécaniser les recherches et gagner un temps considérable dans la recherche

Ordinateur

L’ordinateur permit une plus grande complexification des chiffrements. Par exemple, là ou une machine physique était limitée à 3 rotors, l’ordinateur pouvait en simuler 100 différents.

L’ordinateur permit aussi d’effectuer les opérations plus rapidement. Aussi bien au niveau du chiffrage que du déchiffrage.

Ordinateur

L’ordinateur offre la particularité de travailler sur des nombres et plus sur les lettres de l’alphabet.

Tout est défini au moyen de nombres binaires.

On utilise par exemple le code ASCII pour convertir les caractères en nombres.

Mais on reste malgré tout face à des problèmes de substitution

Ordinateur

L’avantage de travailler avec des bits est que la substitution ne doit plus nécessairement se passer entre 2 lettres, mais peut se passer au sein même d’un bit.

Exemple:

C	H	A	I	S	E
67	72	65	73	83	69
1000011	1001000	1000001	1001001	1010011	1000101
0111100	0110111	0111110	0110110	0101100	0111010
60	55	62	54	44	58
<	7	>	6	,	:

Ordinateur

Mais l’avènement de l’ordinateur mit en lumière 2 problèmes principaux:

- 1 nouveau: la standardisation
- 1 ancien: la distribution de la clé

Ordinateur

Une société pouvait protéger ses communications internes en utilisant le système de cryptage qu'elle voulait

Mais ne pouvait pas communiquer avec une autre société si elles n'utilisaient pas le même système de cryptage

Standardisation

Les tentatives de standardisations des méthodes de cryptage menèrent au développement d'un premier standard appelé DES (Data Encryption Standard).

DES = algorithme de chiffrement symétrique utilisant une clé de 56 bits

Standardisation

L’évolution de la technologie et de la cryptanalyse fait que le DES fut attaqué avec succès et évolua en triple DES (Application du DES 3 fois successivement avec 2 ou 3 clés DES).

Algorithme assez simple à implémenter mais lent.

Standardisation

Le DES et Triple DES sont progressivement remplacés par des systèmes plus modernes: AES

AES = Advanced Encryption Standard

On utilise maintenant des clés de 128 bits à 256 bits

Une attaque par force brute nécessite 2^{128} opérations pour trouver la clé d'un AES-128 ($3{,}4\ 10^{38}$). Certaines méthodes permettent de réduire le nombre d'opérations à $2^{126{,}1}$ ($9{,}1\ 10^{37}$)

Clé publique

Prenons 3 personnes Alice, Bernard et Eve. Alice veut transmettre un message à Bernard. Eve est à l'affut et les espionnes.

Pour crypter ses messages, Alice utilise une clé. Cette clé, elle doit la faire parvenir à Bernard sans que Eve puisse l'intercepter.

Alice et Bernard doivent donc se rencontrer

…

Et s'ils n'avaient pas besoin de se rencontrer ?

Clé publique

Alice veut transmettre un message à Bernard

Elle le place dans une boite qu’elle ferme avec un cadenas à elle

Clé publique

La boite est transmise à Bernard qui ne peut pas l’ouvrir, il ne possède pas la clé du cadenas d’Alice

Il place alors son propre cadenas sur la boite

Clé publique

La boite est à nouveau transmise à Alice. Elle ne peut pas ouvrir le cadenas de Bernard, mais elle peut ouvrir le sien et le retirer

La caisse est toujours protégée par le cadenas de Bernard

Clé publique

La boite est transmise à Bernard qui n’a plus qu’à ouvrir son cadenas pour prendre connaissance du message qu’Alice lui transmet

Clé publique

Eve peut intercepter la boite à tout moment, elle reste fermée par au moins un cadenas qu’elle ne peut pas ouvrir

Clé publique

Appliquons ce principe au message suivant:

la curiosité est un vilain défaut

Clé publique

Alice utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	F	S	U	G	T	A	K	V	D	E	O	Y	J	B	P	N	X	W	C	Q	R	I	M	Z	L

Le chiffrement du message par Alice donne:

Clé publique

Alice utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	F	S	U	G	T	A	K	V	D	E	O	Y	J	B	P	N	X	W	C	Q	R	I	M	Z	L

Le chiffrement du message par Alice donne

L	A	C	U	R	I	O	S	I	T	E	E	S	T	U	N	V	I	L	A	I	N	D	E	F	A	U	T
O	H	S	Q	X	V	B	W	V	C	G	G	W	C	Q	J	R	V	O	H	V	J	U	G	T	H	Q	C

Clé publique

Bernard utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	P	M	G	A	T	N	O	J	E	F	W	I	Q	B	U	R	Y	H	X	S	D	Z	K	L	V

Le chiffrement du message d’Alice par Bernard donne:

Clé publique

Bernard utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	P	M	G	A	T	N	O	J	E	F	W	I	Q	B	U	R	Y	H	X	S	D	Z	K	L	V

Le chiffrement du message d'Alice par Bernard donne:

O	H	S	Q	X	V	B	W	V	C	G	G	W	C	Q	J	R	V	O	H	V	J	U	G	T	H	Q	C
B	O	H	R	K	D	P	Z	D	M	N	N	Z	M	R	E	Y	D	B	O	D	E	S	N	X	O	R	M

Clé publique

Alice utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	F	S	U	G	T	A	K	V	D	E	O	Y	J	B	P	N	X	W	C	Q	R	I	M	Z	L

Le déchiffrement du message de Bernard par Alice donne:

Clé publique

Alice utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	F	S	U	G	T	A	K	V	D	E	O	Y	J	B	P	N	X	W	C	Q	R	I	M	Z	L

Le déchiffrement du message de Bernard par Alice donne

B	O	H	R	K	D	P	Z	D	M	N	N	Z	M	R	E	Y	D	B	O	D	E	S	N	X	O	R	M
O	L	A	V	H	J	P	Y	J	X	Q	Q	Y	X	V	K	M	J	O	L	J	K	C	Q	R	L	V	X

Clé publique

Bernard utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	P	M	G	A	T	N	O	J	E	F	W	I	Q	B	U	R	Y	H	X	S	D	Z	K	L	V

Le déchiffrement du message d’Alice par Bernard donne:

Clé publique

Bernard utilise le chiffre suivant:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	P	M	G	A	T	N	O	J	E	F	W	I	Q	B	U	R	Y	H	X	S	D	Z	K	L	V

Le déchiffrement du message d'Alice par Bernard donne:

O	L	A	V	H	J	P	Y	J	X	Q	Q	Y	X	V	K	M	J	O	L	J	K	C	Q	R	L	V	X
H	Y	E	Z	S	I	B	R	I	T	N	N	R	T	Z	X	C	I	H	Y	I	X	A	N	Q	Y	Z	T

Clé publique

Malheureusement, en cryptologie, ce n’est pas aussi simple…

On est souvent confronté à un ordre bien déterminé pour crypter et décrypter en suivant le principe de dernier arrivé, premier parti,…

Mais l’idée des cadenas va faire son chemin…

Clé publique

Les cryptographes vont commencer à explorer les mathématiques des fonctions à sens unique tel que l'opération **modulo**

Exemple $3^x(mod\ 7)$

x	**1**	**2**	**3**	**4**	**5**	**6**
3^x	3	9	27	81	243	729
$3^x(mod\ 7)$	3	2	6	4	5	1

Clé publique

Exemple $3^x(mod\ 7)$

x	1	2	3	4	5	6	7
3^x	3	9	27	81	243	729	2187
$3^x(mod\ 7)$	3	2	6	4	5	1	3

x	8	9	10	11	12	13	14
3^x	6561	19683	59049	177147	531441	1594323	4782969
$3^x(mod\ 7)$	2	6	4	5	1	3	2

Clé publique

On utilise la fonction $Y^x (mod\ P)$

Alice et Bernard se téléphone et fixe les paramètres $Y = 7$ et $P = 11$

Eve écoute et intercepte ces 2 nombres

Clé publique

Chez elle, Alice choisit un nombre, disons 3, et le garde secret. (Nombre A)	Chez lui, Bernard choisit un nombre, disons 6, et le garde secret (Nombre B)
Alice applique 3 à la fonction à sens unique $7^A(mod\ 11) = 7^3(mod\ 11) = 343(mod\ 11) = 2$	Bernard applique 6 à la fonction à sens unique $7^B(mod\ 11) = 7^6(mod\ 11) = 117649(mod\ 11) = 4$
Alice envoie son résultat à Bernard	Bernard envoie son résultat à Alice
Eve intercepte un des 2 messages ou même les 2 messages	
Alice prend le résultat de Bernard et applique la fonction à sens unique $4^A(mod\ 11) = 4^3(mod\ 11) = 9$	Bernard prend le résultat d'Alice et applique la fonction à sens unique $2^B(mod\ 11) = 2^6(mod\ 11) = 9$
Le résultat obtenu par Alice et Bernard sera utilisé comme clé de chiffrement	
Même en interceptant les nombres d'Alice et de Bernard, Eve n'a pas assez d'information pour reconstruire la clé	

Clé publique

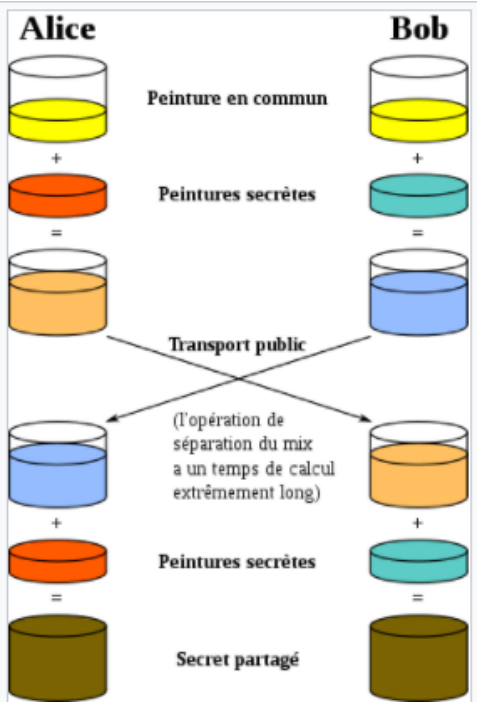
Alice et Bernard peuvent établir une clé secrète tout en conversant publiquement et en ne souciant pas de savoir si les conversations sont écoutées…

Mais le système n’est pas encore idéal, Alice et Bernard doivent se parler. Si Alice vit en Australie et Bernard en Belgique, il faut qu’ils conviennent d’un moment où ils sont éveillés en même temps pour pouvoir échanger les informations de base

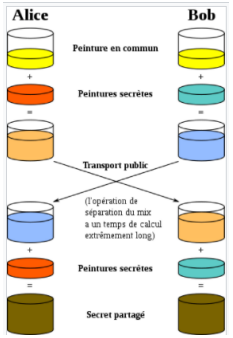
Clé publique

Du point de vue d'Eve, la connaissance des nombres 2 (Alice) et 4 (Bernard) ne l'aide pas à avancer car elle ne connait pas les nombres secrets choisis par Alice et Bernard

Analogie de la peinture …



Clé publique



- Alice et Bob choisissent au préalable une peinture commune, ici le jaune. Cette couleur est connue de tous, y compris de l'intrus Ève.
- Alice choisit une autre couleur secrète (ici du rouge). Elle mélange la peinture commune et sa couleur secrète et obtient de l'orange. Alice envoie la couleur orange à Bob. La couleur orange est connue d'Ève.
- Bob fait de même : il choisit une couleur secrète (ici du cyan) qu'il mélange à la peinture commune et il obtient du bleu. Bob envoie sa couleur bleue à Alice. La couleur bleue est connue d'Ève.
- Alice prend la couleur reçue (le bleu) qu'elle mélange avec sa couleur secrète rouge. Elle obtient une couleur brune.
- Bob prend la couleur reçue (le orange) qu'il mélange avec sa couleur secrète cyan. Il obtient la même couleur brune.

Clé asymétrique

Jusqu'à présent, tous les procédés mentionnés sont basés sur un chiffre à clé **symétrique**

On utilise la clé pour chiffrer et cette même clé est utilisée pour déchiffrer le message

Clé asymétrique

Le principe de clé asymétrique est simple:

Alice crée, chez elle, une clé pour le chiffrement et une clé pour le déchiffrement. Elle rend publique la clé de chiffrement et garde secret la clé de déchiffrement

Bernard veut envoyer un message à Alice. Il prend sa clé de chiffrement publique, chiffre le message et l'envoie à Alice

Alice déchiffre le message avec sa clé de déchiffrement que seule elle connait

RSA

Mais si le principe est simple, il fallut encore des années après l'élaboration du principe de clé asymétrique pour trouver une fonction mathématique qui convenait

On doit la solution au travail de 3 hommes Ron Rivest, Adi Shamir et Leonard Adleman.

Ils trouvèrent une fonction qui était à sens unique, mais qui dans certains cas, pouvait être inversée.

Le système RSA était né

RSA

La fonction du système RSA est basé sur une fonction modulo et sur des nombres premiers

La clé publique est le produit de 2 nombres premiers suffisamment grands

Pour déchiffrer le message, il est nécessaire de connaitre les 2 nombres premiers utilisés pour générer la clé publique

RSA

On peut montrer que si on choisit les 2 nombres premiers 9419 et 1933

Avec une calculatrice, il faut quelques secondes pour trouver le résultat 18206927

Par contre, à partir de ce nombre et d'une calculatrice, il faudrait toute une après-midi pour en extraire les facteurs premiers

RSA

Imaginons que la clé publique est 408508091

Pour trouver les facteurs de ce nombre, il faut tester un à un tous les nombres premiers jusqu'à la solution: 3, 5, 7, 11, ….

Avec une calculatrice pouvant tester 4 nombres à la minute, il faudrait 500 minutes pour trouver les facteurs 18313 et 22307

500 minutes = 8 heures

RSA

Si maintenant les nombres premiers sont des nombres de l'ordre de 10^{65}

La clé publique serait donc un nombre de l'ordre 10^{130}

Il faudrait 50 ans à un ordinateur (en 1995) pour factoriser la clé publique. Et seulement 15 secondes si tous les ordinateurs vendus en 1995 étaient combinés)

Donc on augmenta la taille de la clé à 10^{308}. Il faudrait plus de mille ans à 100 millions d'ordinateur pour factoriser le nombre

RSA

Malheureusement, le système RSA a un problème majeur:

Le chiffrement demande une puissance d'ordinateur que seul les états et l'armée disposaient à cette époque….

RSA – Exemple simplifié

Alice choisit deux nombres premiers p et q.

Disons $p = 17$ et $q = 11$

Note: en pratique, ces nombres devraient être géants

RSA – Exemple simplifié

Alice calcule le produit de ces 2 nombres

$N = p \times q = 17 \times 11 = 187$

Elle doit encore choisir un autre nombre e

Elle choisit $e = 7$

Note: en pratique, il y a des conditions à respecter sur le nombre e

RSA – Exemple simplifié

Alice diffuse les nombre e et N

Ces nombres sont nécessaires pour le chiffrement, ils doivent donc être accessible au public

L'ensemble e et N forme la clé publique d'Alice

RSA – Exemple simplifié

Bernard veut envoyer un message à Alice

Par exemple : rendez-vous dimanche soir

Il convertit tout d'abord ce message en valeur numérique (par exemple au moyen du code ASCII)

R	E	N	D	E	Z	V	O	U	S	D	I	M	A	N	C	H	E	S	O	I	R
82	69	78	68	69	90	86	79	85	83	68	73	77	65	78	67	72	69	83	79	73	82

RSA – Exemple simplifié

Il convertit ensuite chaque code obtenu au moyen de la formule

$$Code = Modulo(Message^{e}; N)$$

Ce qui donne la substitution suivante pour la première lettre

$$R \rightarrow 82 \rightarrow 91$$

R	E	N	D	E	Z	V	O	U	S	D	I	M	A	N	C	H	E	S	O	I	R
82	69	78	68	69	90	86	79	85	83	68	73	77	65	78	67	72	69	83	79	73	82
91	**86**	**56**	**51**	**86**	**95**	**103**	**139**	**68**	**8**	**51**	**61**	**121**	**142**	**56**	**67**	**30**	**86**	**8**	**139**	**61**	**91**

RSA – Exemple simplifié

Alice reçoit donc le message suivant de Bernard

91	86	56	51	86	95	103	139	68	8	51	61	121	142	56	67	30	86	8	139	61	91

Pour le déchiffrer, Alice va à partir des nombres p et q, calculer la clé de déchiffrement d

$$e \times d = 1\big(mod\ (p-1) \times (q-1)\big) = 1\ (mod\ 160)$$
$$7 \times d = 1\ (mod\ 160)$$
$$d = 23$$

RSA – Exemple simplifié

A partir de la clé de déchiffrement, Alice va appliquer la formule suivante:

$$Message = Modulo(Code^{d}; N)$$

Ce qui donne pour la première lettre

$$91 \rightarrow 82 \rightarrow R$$

91	86	56	51	86	95	103	139	68	8	51	61	121	142	56	67	30	86	8	139	61	91
82	69	78	68	69	90	86	79	85	83	68	73	77	65	78	67	72	69	83	79	73	82
R	E	N	D	E	Z	V	O	U	S	D	I	M	A	N	C	H	E	S	O	I	R

RSA – Exemple simplifié

En pratique, il est nécessaire d’avoir recours à un ordinateur pour faire les calculs.

Les nombres sont trop grands pour le faire avec une calculatrice ou même Excel

PGP

Ce problème fut résolu par l'introduction d'un système appelé PGP (Pretty Good Privacy)

Ce système allie la rapidité d'un chiffrement symétrique avec la sécurité d'un chiffrement asymétrique

PGP

Le système PGP offre plusieurs fonctionnalités, mais les 2 principales sont les suivantes:

- Confidentialité: Le message est crypté selon un chiffre symétrique au moyen d'une clé générée aléatoirement par le programme. Cette clé est chiffrée avec un chiffre asymétrique au moyen de la clé publique du destinataire et ajoutée en tête du message
- Authentification: L'expéditeur chiffre un code d'authentification avec sa clé privée (chiffre asymétrique)

Hachage

Fonction de hachage: une fonction particulière qui à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier rapidement la donnée initiale, au même titre qu'une signature pour identifier une personne

Les fonctions de hachage sont utilisées en informatique et cryptographie pour reconnaitre rapidement des fichiers ou des mots de passe

Hachage

Exemple simple:

Pour vérifier si 2 fichiers sont identiques, on peut comparer chaque caractère des 2 fichiers. Mais on peut aussi rapidement vérifier si la taille des fichiers est identique.

Si la taille diffère, les fichiers sont forcément différents

Mais si la taille est identique, on ne peut pas conclure qu'ils sont identiques. La fonction de hachage présente un **taux de collision** trop élevé